HTTP-Anfrage

Ablauf	**Szenario** Auf dem *vmWP1* wird eine die Startseite des Webservers *vmLS2* abgefragt. **Erfassen und Auswerten** Auf *vmLF1* wird der Datenverkehr auf *green0* mit `tcpdump` erfasst und gespeichert. Auf *vmLS2* wir der Datenverkehr auf *eth0* mit *tshark* erfasst und gespeichert. Die Daten werden anschliessend auf den *vmWP1* kopiert und mit *WireShark* angezeigt

Schritt	Maschine	Aktion
1	*vmWP1*	*Chrome* starten und mit der Tastenkombination `Ctrl + Shift + Delete` den Cache löschen
2	*vmWP1* CMD mit Adm	`C:\>arp -d`
3	*vmLF1* Konsole 1	`root@vmLF1:~# ip -s -s neigh flush all` `root@vmLF1:~# tcpdump -i green0 -s 65535 -w /tmp/wp1-http-ls2-lf1.pcap`
4	*vmLS2* Konsole 1	`vmadmin@vmLS2:~$ tshark -i eth0 -w /tmp/wp1-http-ls2-ls2.pcap`
5	*vmWP1*	Im *Chrome* http://192.168.220.11 aufrufen
6	*vmLF1* und *vmLS2*	Aufzeichnungen mit `Ctrl+C` abbrechen
7	*vmWP1*	Aufzeichnungen von *vmLF1* und *vmLS2* ins Verzeichnis `C:\capdat` kopieren.
8	*vmWP1*	`wp1-http-ls2-lf1.pcap` und `wp1-http-ls2-ls2.pcap` je mit *WireShark* öffnen
9	*vmWP1*	In beiden Fenster den Display-Filter `arp` setzen und `Apply` drücken.

Fragen	Welche Protokolle benutzt `arp`?	`- ethernet und arp`
	Wie unterscheiden sich die `arp`-Broadcasts in den zwei Auswertungen?	`- MAC von vmWP1 frägt MAC von vmLF1 green0` `- MAC vmLF1 orange0 frägt MAC von vmLS2`

Schritt	Maschine	Aktion
10	*vmWP1*	Setzen Sie den Display-Filter je auf **`ip.dst == 192.168.220.11 && http`**

Fragen	Was bewirkt der gesetzte Filter?	`es werden nur Pakete mit der Ziel-IP 192.168.220.11 mit http-Anwendungsanfragen angezeigt`
	Auf welcher Schicht unterscheiden sich die Einträge aus den zwei Dateien? Begründen Sie Ihre Antwort.	`Netzzugangsschicht. Die MAC-Adressen sind bei den gleichen Sätzen verschieden. Einmal vmWP1 -> vmLF1, dann vmLF1 -> vmLS2`
	Skizzieren Sie den Datenverkehr der Webanfrage (*vmWP1 -> vmLF1 –> vmLS2*) durch die TCP/IP-Schichten.	

TCP/IP-Modell